## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently amended) A method that facilitates sharing authentication information between a plurality of servers within a distributed computing system, wherein the plurality of servers includes a first server and an authentication server, the method comprising:

receiving a communication from a client at the first server;

determining whether the client is known to the first server; and

if the client is unknown to the first server,

generating a first identifier for the client,

communicating the first identifier to the client, and

directing the client to communicate the first identifier to the authentication server, so that the authentication server can attempt to associate the first identifier with a known client~~, thereby authenticating the client without requiring a user to enter the username and password again~~,

if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client; thereby authenticating the client without requiring the authentication server to receive authentication data from the client.

2. (Currently amended) The method of claim 1,

~~wherein if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client;~~

wherein if the client is unknown to the authentication server, the authentication server causes the client to store a cookie for the authentication server, wherein the cookie contains an identifier for the client, so that the authentication server can subsequently identify the client by examining the cookie.

3. (Original) The method of claim 1, wherein the authentication server determines whether or not the client is known to the authentication server by attempting to examine a cookie presented by the client to the authentication server.

4. (Original) The method of claim 1, wherein if the client is unknown to the first server, the method additionally comprises causing the client to store a cookie for the first server, so that the client can subsequently present the cookie to the first server in order to identify the client to the first server.

5. (Original) The method of claim 1, further comprising:

receiving a username and a password from the client;

attempting to authenticate the client based on the username and the password; and

if the client authenticates, associating the username with the client.

6. (Original) The method of claim 1, wherein determining whether the client is known to the first server involves:

looking for a cookie presented by the client to the first server; and

if such a cookie is presented by the client, determining if the cookie contains an identifier that is known to the first server.

7. (Currently amended) A method that facilitates sharing authentication information between a plurality of servers within a distributed computing system, wherein the plurality of servers includes a first server and an authentication server, the method comprising:

receiving a communication from a client at the authentication server, wherein the communication includes a first identifier generated by the first server for the client;

determining whether the client is known to the authentication server;

if the client is known to the authentication server, associating the first identifier with a pre-existing identifier for the client; ~~and~~

if the client is unknown to the authentication server, causing the client to store a cookie for the authentication server, wherein the cookie contains an identifier for the client, so that the authentication server can subsequently identify the client by examining the cookie~~, thereby authenticating the client without requiring a user to enter the username and password again~~; and

if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client; thereby authenticating the client without requiring the authentication server to receive authentication data from the client.

8. (Original) The method of claim 7, wherein the authentication server determines whether or not the client is known to the authentication server by attempting to examine a cookie presented by the client to the authentication server.

9. (Original) The method of claim 7, further comprising:

receiving a username and a password from the client;

attempting to authenticate the client based on the username and the password; and

if the client authenticates, associating the username with the client.

10. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method that facilitates sharing authentication information between a plurality of servers within a distributed computing system, wherein the plurality of servers includes a first server and an authentication server, the method comprising:

receiving a communication from a client at the first server;

determining whether the client is known to the first server; and

if the client is unknown to the first server,

generating a first identifier for the client,

communicating the first identifier to the client, and

directing the client to communicate the first identifier to the authentication server, so that the authentication server can attempt to associate the first identifier with a known client~~, thereby authenticating the client without requiring a user to enter the username and password again~~,

if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client; thereby authenticating the client without requiring the authentication server to receive authentication data from the client.

11. (Currently amended) The computer-readable storage medium of claim 10,

~~wherein if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client;~~

wherein if the client is unknown to the authentication server, the authentication server causes the client to store a cookie for the authentication server, wherein the cookie contains an identifier for the client, so that the authentication server can subsequently identify the client by examining the cookie.

12. (Original) The computer-readable storage medium of claim 10, wherein the authentication server determines whether or not the client is known to the authentication server by attempting to examine a cookie presented by the client to the authentication server.

13. (Original) The computer-readable storage medium of claim 10, wherein if the client is unknown to the first server, the method additionally comprises causing the client to store a cookie for the first server, so that the client can subsequently present the cookie to the first server in order to identify the client to the first server.

14. (Original) The computer-readable storage medium of claim 10, wherein the method further comprises:

receiving a username and a password from the client;

attempting to authenticate the client based on the username and the password; and

if the client authenticates, associating the username with the client.

15. (Original) The computer-readable storage medium of claim 10, wherein determining whether the client is known to the first server involves:

looking for a cookie presented by the client to the first server; and

if such a cookie is presented by the client, determining if the cookie contains an identifier that is known to the first server.

16. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method that facilitates sharing authentication information between a plurality of servers within a distributed computing system, wherein the plurality of servers includes a first server and an authentication server, the method comprising:

receiving a communication from a client at the authentication server, wherein the communication includes a first identifier generated by the first server for the client;

determining whether the client is known to the authentication server;

if the client is known to the authentication server, associating the first identifier with a pre-existing identifier for the client; ~~and~~

if the client is unknown to the authentication server, causing the client to store a cookie for the authentication server, wherein the cookie contains an identifier for the client, so that the authentication server can subsequently identify the client by examining the cookie~~, thereby authenticating the client without requiring a user to enter the username and password again~~; and,

if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client; thereby authenticating the client without requiring the authentication server to receive authentication data from the client.

17. (Original) The computer-readable storage medium of claim 16, wherein the authentication server determines whether or not the client is known to the authentication server by attempting to examine a cookie presented by the client to the authentication server.

18. (Original) The computer-readable storage medium of claim 16, wherein the method further comprises:

receiving a username and a password from the client at the first server;

attempting to authenticate the client based on the username and the password; and

if the client authenticates, associating the username with the client.

19. (Currently amended) An apparatus that facilitates sharing authentication information between a plurality of servers within a distributed computing system, the apparatus comprising:

a first server within the plurality of servers;

a receiving mechanism within the first server that is configured to receive a communication from a client; and

an identification mechanism within the first server that is configured to determine whether the client is known to the first server;

wherein if the client is unknown to the first server, the identification mechanism is configured to,

generate a first identifier for the client,

communicate the first identifier to the client, and to

direct the client to communicate the first identifier to the authentication server, so that the authentication server can attempt to associate the first identifier with a known client~~, thereby authenticating the client without requiring a user to enter the username and password again~~;

wherein if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client; thereby authenticating the client without requiring the authentication server to receive authentication data from the client.

20. (Currently amended) The apparatus of claim 19, further comprising

an authentication server within the plurality of servers;

an association mechanism within the authentication server;

~~wherein if the client is known to the authentication server, the association mechanism is configured to associate the first identifier with a pre-existing identifier for the client;~~

wherein if the client is unknown to the authentication server, the association mechanism is configured to cause the client to store a cookie for the authentication server, wherein the cookie contains an identifier for the client, so that the authentication server can subsequently identify the client by examining the cookie.

21. (Original) The apparatus of claim 20, wherein the authentication server additionally includes an identification mechanism that is configured to determine whether or not the client is known to the authentication server by attempting to examine a cookie presented by the client to the authentication server.

22. (Original) The apparatus of claim 19, wherein if the client is unknown to the first server, the identification mechanism is additionally configured to cause the client to store a cookie for the first server, so that the client can subsequently present the cookie to the first server in order to identify the client to the first server.

23. (Original) The apparatus of claim 19, further comprising an authentication mechanism that is configured to:

receive a username and a password from the client;

attempt to authenticate the client based on the username and the password; and to

associate the username with the client if the client authenticates.

24. (Original) The apparatus of claim 19, wherein the identification mechanism is configured to:

look for a cookie presented by the client to the first server; and

if such a cookie is presented by the client, to determine if the cookie contains an identifier that is known to the first server.

25. (Currently amended) An apparatus that facilitates sharing authentication information between a plurality of servers within a distributed computing system, the apparatus comprising:

an authentication server within the plurality of servers;

a receiving mechanism within the authentication server that is configured to receive a communication from a client, wherein the communication includes a first identifier generated by a first server within the plurality of servers for the client;

an identification mechanism within the authentication server that is configured to determine whether the client is known to the authentication server; and

an association mechanism within the authentication server;

wherein if the client is known to the authentication server, the association mechanism is configured to associate the first identifier with a pre-existing identifier for the client;

wherein if the client is unknown to the authentication server, the association mechanism is configured to cause the client to store a cookie for the authentication server, wherein the cookie contains an identifier for the client, so that the authentication server can subsequently identify the client by examining the cookie~~, thereby authenticating the client without requiring a user to enter the username and password again~~; and

wherein if the client is known to the authentication server, the authentication server associates the first identifier with a pre-existing identifier for the client; thereby authenticating the client without requiring the authentication server to receive authentication data from the client.

26. (Original) The apparatus of claim 25, wherein the identification mechanism is configured to determine whether or not the client is known to the authentication server by attempting to examine a cookie presented by the client to the authentication server.

27. (Original) The apparatus of claim 25, further comprising an authentication mechanism that is configured to:

receive a username and a password from the client;

attempt to authenticate the client based on the username and the password; and to

associate the username with the client if the client authenticates.